Principles and Foundations for Fractionated Networked Cyber-Physical Systems

Quarterly Report

Mark-Oliver Stehr Pat Lincoln

Date of Preparation: 10/14/2010
Period covered: Inception - 9/30/2011

Project Abstract A new generation of mission-critical systems is emerging that employs distributed, dynamically reconfigurable open architectures. These systems may include a variety of devices that sense and affect their environment and the configuration of the system itself. We call such systems *Networked Cyber-Physical Systems* (NCPS). NCPS can provide complex, situation-aware, and often critical services in applications such as distributed sensing and surveillance, crisis response, self-assembling structures or systems, networked satellite and unmanned vehicle missions, or distributed critical infrastructure monitoring and control. NCPS are of special interest to the Navy in view of the increasing need for coordination of a wide spectrum of maritime sensing and information gathering technologies, ranging from smart mobile buoys to autonomous underwater vehicles and their integration into a global network with maritime, space, and ground domains.

NCPS must be reactive and maintain an overall situation, location, and time awareness that emerges from the exchange of knowledge. They must achieve system goals through local, asynchronous actions, using (distributed) control loops through which the environment provides essential feedback. They must deal with uncertainty and partial knowledge, and be capable of a wide spectrum of operations between autonomy and cooperation to adapt to resource constraints and disruptions in communication. General principles and tools are needed for building robust, effective NCPS. A key observation is that the current level of abstraction at which software and systems are designed is a barrier to innovation at the hardware and networking level and at the same time is not suitable to enable rapid design/deployment or distributed control of large-scale distributed software

systems and in particular the flexible, dynamically reconfigurable, mission-critical NCPS of the future.

We propose to explore a new paradigm for design of high-assurance NCPS based on the notion of software fractionation with declarative distributed control and optimization aiming at the effective use of resources. The idea of software fractionation is inspired by and complementary to hardware fractionation, which has been proposed for mission-critical space systems. Fractionation has the potential of leading to software that is more robust, leveraging both diversity and redundancy. It raises the level of abstraction at which control and optimization techniques are applied.

1 Technical Approach

In this project we adopt a view of cyber-physical systems that goes beyond the conventional definition of a hardware/software system that is interacting with the physical world. Our goal is to explore a new notion of software that behaves itself closer to a physical or biological system. In other words, we aim to address the fundamental problem by reducing the sharp boundary between physics and computation. Our rationale is that current models of distributed computing are too abstract by not taking into account fundamental physical limitations and hence are not efficiently implementable or scalable. Once limitations can be explicitly represented, they can be overcome to some degree, which can be quantified, e.g. probabilistically. Like in biological systems, diversification, redundancy, and randomization should be utilized to overcome physical limitations whenever possible. In particular, distribution is a source of redundancy and diversification that can be turned from an obstacle into an advantage.

In our approach, software is fractionated by design even beyond the distributed nature of underlying system, with distributed knowledge sharing as the underlying model. Computation and communication is not rigid but guided by the physical resources, e.g. in an opportunistic fashion. Our vision that fractionated software operates as an inherently open system in a highly redundant and diversified way avoiding single points of responsibilities and failure. Being resource-aware, fractionated software operates in the entire spectrum between autonomy to cooperation. Our distributed computing model is based on distributed knowledge sharing, and makes very few assumptions but restricts the shape of fractionated software so that it can run on a wide range of platforms. In particular it does not assume strong primitives that are powerful but not implementable in a scalable way.

2 Activities during this Quarter

After an interruption of our work after the end of Phase 1, we are continuing our work as planned to proceed with Phase 2. During this quarter we have conducted research on two related foundational aspects of fractionated NCPS and also supported the development of an NCPS testbed at SRI.

2.1 Research on Foundations

The vision of fractionated software is that distributed computations are mapped to resources at runtime in a flexible way without the need for a complex (global) coordination mechanism. If some components fail other components can step in and take over the computation without the need for explicit migration. Randomization techniques will make sure that enough diversity is maintained to allows reasonably efficient operation, e.g. to achieve performance and reliability constraints.

The underlying distributed computing model has been developed under the name Partially Ordered Knowledge Sharing, which allows very loosely coupled operation that can be effective even in situations of continuous failures of network or computational elements as they may especially occur in hostile environments.

For a more concrete and more declarative model of fractionated software we are currently developing a distributed dataflow model on top of partially ordered knowledge sharing. The objective is to allow the programmer to explicitly specify the data objects and functions so that a runtime system can execute the dataflow description in a distributed self-coordinating fashion. As a starting point we use Petri nets (specifically Colored Petri nets), which are well-known and can explicitly represent the dataflow, but they need to be adapted to allow for truly distributed computations in the fractionated sense, which is the main challenge of this line of work.

The resulting model is not only suitable to represent dataflow but also control flow, e.g. for distributed control of fractionated systems. Currently, we are investigating the distributed control of ensembles (specifically UAV swarms) as an interesting application. Our work uses a declarative approach based on virtual potential functions, in which distributed control can be expressed as an optimization problem. Specifically, we explored a fractionated version of distributed surveillance (e.g., utility optimization and mapping can be performed by different UAVs in parallel) on top of our Parallel and Distributed Optimization framework. The integration of virtual potential functions with our new distributed data and control flow model is planned for the next quarter, and can be expected to give rise to a new paradigm for the design of fractionated software/systems of many kinds.

2.2 Work on NCPS Testbed

In parallel with the foundational work, which we are testing in a simulation environment, we are also developing a small UAV testbed at SRI, which can be used to conduct real-world experiments. The hardware is based on inexpensive quadricopter technology, which we are currently modifying to allow for more autonomy and improved capabilities such as localization in physical space. We are currently focusing on improving the sensing capabilities of individual nodes and the development of suitable control software, and we expect to continue this work during the next quarter, before we move to the multi-quadricopter case.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*
10/14/2011

2. REPORT TYPE
Quarterly Report - Phase 2

3. DATES COVERED *(From - To)*
Inception - 09/30/11

4. TITLE AND SUBTITLE
Principles and Foundations for Fractionated Networked Cyber-Physical Systems

5a. CONTRACT NUMBER

5b. GRANT NUMBER
N00014-10-1-0365

5c. PROGRAM ELEMENT NUMBER

5d. PROJECT NUMBER
11PR00456-05

5e. TASK NUMBER

5f. WORK UNIT NUMBER

6. AUTHOR(S)
Dr. Mark-Oliver Stehr
Dr. Patrick Lincoln

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
SRI International
333 Ravenswood Avenue
Menlo Park, CA 94025-3493

8. PERFORMING ORGANIZATION REPORT NUMBER
P20679Qrt 1

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Office of Naval Research
875 North Randolph Street
Arlington, VA 22203-1995

10. SPONSOR/MONITOR'S ACRONYM(S)
ONR

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for Public Release, Distribution is Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT
We propose to explore a new paradigm for design of high-assurance Networked Cyber-Physical Systems based on the notion of software fractionation with distributed control and optimization aiming at the effective use of resources. The idea of software fractionation is inspired by and complementary to hardware fractionation, which has been proposed for mission-critical space systems. In our approach, software is fractionated by design even beyond the distributed nature of underlying system, with distributed knowledge sharing as the underlying model. In this report we briefly summarize our research on foundations for distributed dataflow and control of fractionated systems as well as our work on building an NCPS testbed at SRI.

15. SUBJECT TERMS
Fractionated Software, Distributed Computing, Networking, Cyber-Physcial Systems

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**	uu		Kathryn Tracy
u	u	u			**19b. TELEPHONE NUMBER** *(Include area code)* 650-859-3435